Sen. Mathias on the Data Banks

The following is excerpted from testimony given Tuesday by Sen. Charles McC. Mathias (R-Md.) before the Senate Judiciary Subcommittee on Constitutional Rights: 3/14/71

MR. CHAIRMAN, I appreciate the opportunity to appear today to make whatever contributions I can to your inquiry into governmental data banks and the very serious constitutional and policy questions involved.

This inquiry is constructive and overdue. As your investigations have dramatized, our basic freedoms—the right of privacy, freedom of speech, freedom of association—are at the mercy of an amoral technology. Thanks to "good old American know-how," we now know how to find out so much about each other that we are in imminent danger of trampling what Justice Brandeis called "the right most valued by civilized men, the right to be let alone." . . .

I would like to focus . . . on the problems of controlling data and data banks in one particular area: the field of law enforcement and the administration of justice. Clearly in this area, more than in many others, there is a legitimate need for public agencies to have considerable information about individuals. At the same time, there is an especially urgent need to protect individuals against arbitrary or excessive exercises of the awesome police powers of the state.

In some instances equity may require police or courts to know more, rather than less, about an individual. For instance, when John Q. Public is being sentenced following conviction, it is not enough for the sentencing judge to know that Mr. Public has a record of five previous arrests. The judge should also know whether these arrests were for speeding or for assault, and what disposition was made of each charge.

On the other hand, Mr. Public should have some assurance that a youthful indiscretion will not follow him all the days of his life. For example, if a youth receives a suspended sentence at age 18 for repossession of marijuana, or for involvement in a campus demonstration, that fact could pop up for years to jeopardize his applications for jobs, for credit cards and for home loans.

As one grim example, the Bureau of Narcotics and Dangerous Drugs (BNDD) maintains computerized files on narcotic users. As of Oct. 30, 1970, those files covered over 64,000 individuals—including three boys under 3 years old! Will that item be buried in statistical reports, surfacing only as a curiosity? Or will three boys be pursued for life by the tragic fact that they were exposed to narcotics almost before they could talk?

WE ARE now witnessing a tremendous surge in the development and use of computerized data banks by law enforcement agencies throughout the nation. Although no single, nationwide federal-state-local system for collecting and transmitting personal histories has yet been established, all signs show that law enforcement agencies are hurtling in this direction, fueled largely by federal funds and unrestrained by any consistent controls.

Within the Department of Justice, there are several large, active computerized data banks: the FBI's National Crime Information Center on wanted persons; the BNDD files on narcotics users; the FBI's Known Professional Check Passers File; the Organized Crime Intelligence System; a file on offenders, based on federal penitentiary records; and the records of the Immigration and Naturalization Service . . .

While each of these data banks is currently separately maintained, the contents of each—with the exception of some intelligence data—is made available when needed not just within the Justice Department, but also to other federal agencies with even marginal law enforcement mandates, to state and local agencies, and in some cases to private establishments such as national banks. The federal stamp of course gives all such data the force and validity of gospel. Federal law, in fact, encourages the collection and exchange of criminal records under the aegis of law enforcement.

At the same time that these federal files are growing, nearly every state and many cities are establishing their own data banks, often with funds provided under the Safe Streets Act of 1968 . . .

State and local law enforcement agencies do not necessarily have any fewer scruples than federal bureaus about keeping personal histories confidential, or about jealously guarding criminal intelligence and raw investigatory files. But computers are bringing the ammunition for persecution, harassment and idle gossip within the reach of every prosecutor and part-time deputy sheriff in the land . . .

It is encouraging that the most extensive new data system, Project SEARCH, has also been extremely sensitive to problems of individual privacy. Project SEARCH is the 10-state System for Electronic Analysis and Retrieval of Criminal Histories which in December completed an 18-month demonstration period at a combined federal-state cost of $2.5 million. During that period, the SEARCH Project Group developed not only the technical capacity to collect and exchange standardized criminal histories, but also an impressive code of ethics . . .

The philosophy summarized in this code of ethics is amplified in Technical Report No. 2, prepared by the Project SEARCH Committee on Security and Privacy. Among other steps, this report prescribes procedures for

—limiting data to that "with the characteristics of public records," recorded "only upon the report of a crime," and excluding such irrelevant data and unreliable material as unverified intelligence tips;

—continuously re-evaluating included data for its accuracy and completeness, and purging such items as "the record of first offenders where criminal proceedings have resulted in a determination in favor of such persons";

—developing a "high level of computer,

legal, physical, information, communications, and personnel security methods" to protect the system and give full protection to all information included; and

—developing "procedures for an individual to learn the contents of the arrest record kept about him and for the correction of inaccuracies or prejudicial omissions in a person's arrest record."

Overall, Technical Report No. 2 is a perceptive, challenging and generally successful attempt to come to grips with the problems inherent in an efficient, nationwide criminal justice data bank.

Obviously, this approach has its critics. For instance, after reviewing an early draft of Technical Report 2, an FBI spokesman called it "very objectionable."

On Dec. 9, 1970, LEAA approved a new grant of $1,552,060 to Project SEARCH for calendar year 1971 "to further develop and make operational an offender-record based criminal justice information system." On Dec. 19, 1970, in an internal directive which was *not* publicly released, the Attorney General transferred the prime responsibility for future development of a nationwide system for exchanging criminal histories from LEAA to the FBI. I have been advised that this brief letter made no reference to privacy issues or the fate of the standards so carefully shaped by the SEARCH Project Group. Nor was the FBI's new mandate mentioned at all when the LEAA grant to Project SEARCH was routinely announced on Dec. 16.

THESE EVENTS add up to a quantum jump toward a national criminal justice data bank — a leap taken without full public knowledge or specific congressional authorization. It will probably be touted as a great advance for law enforcement. It may also be feared as a tremendous threat to individual rights.

Mr. Chairman, we should act now to establish reasonable rules to govern such operations. Some argue that the needs of law enforcement are so great that new technology should not be fettered by precious concerns for the niceties of privacy. Others assert that any regulatory efforts in this field are an unwarranted reflection on the integrity of our hallowed system of criminal justice. Still others maintain that the regulatory chore should be left to the states, as it was in the days when a criminal record could be transmitted across the country only by mail.

In response we must consider Juvenal's question: *Sed quis custodiet ipsos custodes?* But who guards the guardians? . . .

As I have suggested, these criteria embrace a vast and mushrooming field. By enacting definite standards for federal data banks, Congress can inject order into operations now subject to great misunderstanding and suspicion, and promote public confidence in those data collection systems which are necessary. By imposing basic requirements on other systems involving federal funds or linkages, Congress can guide the states and take a long step toward insuring that any state or local data bank abuses or excesses will remain localized . . .

In conclusion . . . I do not believe that we are doomed to perpetual war between computers and the Constitution. Rather, I am confident that—through hard work and constant watchfulness—we can civilize our technology so as to promote both justice and liberty. I look forward to working with you toward that goal.